Appendix A

```
<SigningRequest Return="Signature">
     <Policy>
        <SignatureInfo Type="detached"/>
        <KeyInfo>
            <KeyName
Type="email_name">rsalz@zolera.com</KeyName>
        </KeyInfo>
        <CertChain Length="All" Type="Certificate"/>
    </Policy>
    <Document URI="url of document" />
</SigningRequest>
```

Appendix B

```
<SigningRequest>
     <Policy>
        <SignatureInfo Type="enveloped"/>
        <KeyInfo>
            <X509Data>
                 <X509IssuerSerial>
                    <X509IssuerName>CN=Rich Salz, O=Zolera, C=US
                    </X509IssuerName>
                    <X509SerialNumber>12345678</X509SerialNumber>
                 </X509IssuerSerial>
             </X509Data>
        </KeyInfo>
        <CertChain Length="All" Type="Certificate"/>
    </Policy>
  <Document URI="url of document"
Algorithm="http://www.w3.org/2000/09/xmldsig#base64">
        base64 encoded document
    </Document>
</SigningRequest>
```

Appendix C

```
<purchaseOrder orderDate="1999-10-20">
    <items>
        <item partNum="872-AA">
            <productName>Lawnmower</productName>
            <quantity>1</quantity>
            <USPrice>148.95</USPrice>
        </item>
    </items>
</purchaseOrder>
```

Appendix D

```
<SigningRequest Return="Signature">
     <Policy>
        <SignatureInfo Type="enveloped"/>
        <KeyInfo>
            <KeyName
Type="email_name">rsalz@zolera.com</KeyName>
        </KeyInfo>
        <CertChain Length="None"/>
    </Policy>
    <Document URI="po_txn_123">
         <purchaseOrder orderDate="1999-10-20">
            <items>
                <item partNum="872-AA">
                    <productName>Lawnmower</productName>
                    <quantity>1</quantity>
                    <USPrice>148.95</USPrice>
                </item>
            </items>
        </purchaseOrder>
    </Document>
</SigningRequest>
```

Appendix E

```
<purchaseOrder orderDate="1999-10-20">
    <items>
        <item partNum="872-AA">
            <productName>Lawnmower</productName>
            <quantity>1</quantity>
            <USPrice>148.95</USPrice>
        </item>
    </items>
    <Signature Id="178ae4" xmlns="http://www.w3.org/2000/09/xmldsig#">
         <SignedInfo>
         <SignatureMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
             <Reference URI="">

      <DigestMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <DigestValue>j61wx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
              </Reference>
                   <Reference
      URI="#ServerSignatureProperties"Type="http://www.w3.org/2000/09/xm
      ldsig#SignatureProperty">
      <DigestMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <DigestValue>k3453rvEPO0vKtMup4NbeVu8nk=</DigestValue>
            </Reference>
            <Reference URI="#KeyInfo">
      <DigestMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <DigestValue>7abc3rvEPO0vKtMupdefVxdu8nk=</DigestValue>
            </Reference>
         </SignedInfo>
        <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
        <KeyInfo Id="KeyInfo">
            <KeyNameType="email_name">rsalz@zolera.com</KeyName>
        </KeyInfo>
        <Object>
            <SignatureProperties>
                  <SignaturePropertyId="ServerSignatureProperties">
                        <ServerInfoxmlns="urn:caveosystems:sign1">
          <ServerIdentifier>hancock serveridentifier</ServerIdentifier>
     <SignatureReference>AB14E72
</SignatureReference>

<AuthenticityStamp>blob</AuthenticityStamp>
<VerificationURI>http://www.zolera.com/2000/VerifierService/
</VerificationURI>
      </ServerInfo>
<timestamp xmlns="http://www.ietf.org/rfcXXXX.txt">YYYYMMDDHHMMSS.fffZ
</timestamp>
                </SignatureProperty>
            </SignatureProperties>
        </Object>
    </Signature>
</purchaseOrder>
```

Appendix F

```
            <SigningResponse>
                <Status Type="Success"/>
                <SignatureResult Return="Signature">
                    <Signature Id="178ae4" xmlns="http://www.w3.org/2000/09/xmldsig#">
                        <SignedInfo>
                            <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                            <Reference URI="">
                                <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
                                </Reference>
                           <Reference
URI="#ServerSignatureProperties"Type="http://www.w3.org/2000
                                /09/xmldsig#SignatureProperty">
                    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                     <DigestValue>k3453rvEPO0vKtMup4NbeVu8nk=</DigestValue>
                         </Reference>
                    <Reference URI="#KeyInfo">

<DigestMethodAlgorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                     <DigestValue>7abc3rvEPO0vKtMupdefVxdu8nk=
                    </DigestValue>
                     </Reference>
                     </SignedInfo>
                     <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
                        <KeyInfo Id="KeyInfo">
                     <KeyName Type="email_name">rsalz@zolera.com</KeyName>
                        </KeyInfo>
                        <Object>
                             <SignatureProperties>
              <SignatureProperty Id="ServerSignatureProperties"
                               <ServerInfo
        xmlns="urn:caveosystems:sign1">          <ServerIdentifier>hancock
        server identifier</ServerIdentifier>
              <SignatureReference>AB14E72
            </SignatureReference>
               <AuthenticityStamp>blob</AuthenticityStamp>

<VerificationURI>http://www.zolera.com/2000/VerifierService/</VerificationURI>
              </ServerInfo>
            <timestamp xmlns="http://www.ietf.org/rfcXXXX.txt">
                         YYYYMMDDHHMMSS.fffZ</timestamp>
          </SignatureProperty>
               </SignatureProperties>
                     </Object>
                   </Signature>
                </SignatureResult>
            </SigningResponse>
```

Appendix G

```
<VerificationRequest Type="receipt">
    <VerifyInfo>
            <Signature>
            The XML signature to be verified, including
SignedInfo and Objects. Hancock Signature Object and
KeyInfo required.
            </Signature>

            <Document URI="url of document"
Algorithm="http://www.w3.org/2000/09/xmldsig#base64">
               base64 encoded document
            </Document>
 </VerificationRequest>
```

Appendix H

```
<VerificationRequest>
    <VerifyInfo>
            <Signature Id="7"/>
            <Document
URI="http://www.zolera.com/example.xml"/>
    </VerifyInfo>
</VerificationRequest>
```

Appendix I

```
<VerificationResponse>
    <VerifyInfo>
        <SignatureReference Type="Id">7</SignatureReference>
     <SignatureStatus Type="Invalid"/>
     <CredentialStatus Type="Revoked"
Type="Certificate">MIICPzCCA...</CredentialStatus>
   </VerifyInfo>
    <ServerIdentifier>75axxx</ServerIdentifier>
    <Timestamp></Timestamp>
</VerificationResponse>
```

Appendix J

```
<VerificationResponse TYPE="receipt">
      elements as defined above, and additional Signature
elements:
      <Signature>
        <SignedInfo </SignedInfo>
        <Object>
            <SignatureProperties>
                <SignatureProperty
Id="ServerSignatureProperties"> as defined above
                </SignatureProperty>
            </SignatureProperties>
        </Object>
    </Signature> </VerificationResponse>
```

Appendix K

```
<SignatureSummaryRequest>
            <SignedDocument URI="url of document"
Algorithm="http://www.w3.org/2000/09/xmldsig#base64">
               base64 encoded document
            </SignedDocument>
</SignatureSummaryRequest>
```

Appendix L

```
<SignatureSummaryRequest>
            <SignedDocumentIdentifier
>7E5</SignedDocumentIdentifier>
            <SignatureIdentification Id="78"/>
</SignatureSummaryRequest>SignedDocumentIdentifier
```

Appendix M

```
<SignatureSummary >
    <SignatureInfo Id="firstsig" TYPE="detached">
        <KeySummary Length="56" Rating="B"/>
           <SignatureSummary
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
Rating="C+"/>
        <CredentialSummary Type="none" Rating="F"/>
    <SignatureInfo>
     <SignatureInfo Id="secondsig" TYPE="enveloped">
        <KeySummary Length="128" Rating="A"/>
        <SigSummary
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
Rating="A"/>
        <CredentialSummary Type="x509"  Rating="c">
            <X509Data> <!-- certificate chain -->
               <!--Signer cert, issuer
C=US,O=IBM,OU=FVT,CN=arbolCA serial 4-->
               <X509Certificate>MIICXTCCA..</X509Certificate>
                   <!-- Intermediate cert subject
C=US,O=IBM,OU=FVT,CN=arbolCAissuer,C=US,O=Bridgepoint,OU=FVT,CN=tootiseCA -->
               <X509Certificate>MIICPzCCA...</X509Certificate>
               <!-- Root cert subject
C=US,O=Bridgepoint,OU=FVT,CN=tootiseCA -->
               <X509Certificate>MIICSTCCA...</X509Certificate>
                  <!-- Root cert subject
C=US,O=Bridgepoint,OU=FVT,CN=tootiseCA -->
               <X509Certificate>MIICSTCCA...</X509Certificate>
             </X509Data>
        </CredentialSummary>
    <SignatureInfo>
    <Disclaimer>text</Disclaimer>
</SignatureSummary>
```

Appendix N

```
<Signature>
    <SignedInfo>
        (CanonicalizationMethod)
        (SignatureMethod)
        (<Reference (URI=)? >
            (Transforms)?
            (DigestMethod)
            (DigestValue)
        </Reference>)+
    </SignedInfo>
    (SignatureValue)
    (KeyInfo)?
    (Object)*
</Signature>
```

Appendix O

```
<Reference URI="http://www.w3.org/TR/2000/REC-xhtml1-20000126/">
    <Transforms>
         <Transform Algorithm="http://www.w3.org/TR/2000/WD-xml-c14n-20000710"/>
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
</Reference>
```

Appendix P

```
<KeyInfo>
     <X509Data> <!-- certificate chain -->
       <!--Signer cert, issuer C=US,O=IBM,OU=FVT,CN=arbolCA serial 4-->
       <X509Certificate>MIICXTCCA..</X509Certificate>
       <!-- Intermediate cert subject C=US,O=IBM,OU=FVT,CN=arbolCA
issuer,C=US,O=Bridgepoint,OU=FVT,CN=tootiseCA -->
       <X509Certificate>MIICPzCCA...</X509Certificate>
       <!-- Root cert subject C=US,O=Bridgepoint,OU=FVT,CN=tootiseCA -->
       <X509Certificate>MIICSTCCA...</X509Certificate>
     </X509Data>
 </KeyInfo>
```

Appendix Q

```xml
<Object>
    <SignatureProperties>
        <SignatureProperty Id="ServerSignatureProperties">
            <HancockSignatureProperties></HancockSignatureProperties>
        </SignatureProperty>
    </SignatureProperties>
</Object>
```

Appendix R

```xml
<Reference URI="#ServerSignatureProperties"
Type="http://www.w3.org/2000/09/xmldsig#SignatureProperty">
   <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
   <DigestValue>k3453rvEPO0vKtMup4NbeVu8nk=</DigestValue>
</Reference>
```

Appendix S

```
POST /SigningRequest HTTP/1.1
Host: www.signingserver.com
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn
SOAPAction: "Some-URI"

<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/en
coding/">
   <SOAP-ENV:Body>
       <SigningRequest Return="Signature"
xmlns:"urn:caveosystems:sign1">
             <Policy>
                <SignatureInfo Type="detached"/>
                <KeyInfo>
                    <KeyName
Type="email_name">rsalz@zolera.com</KeyName>
                </KeyInfo>
                <CertChain Length="All" Type="Certificate"/>
            </Policy>
            <Document URI="url of document" />
        </SigningRequest>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```